SERENA FORDHAM ENTERPRISES LTD, FOR HER GROUP LTD & NORFOLK MUMS

Information Security Policy

INFORMATION SECURITY POLICY

Table of Contents:

1. Document Control 4
2. Introduction 5
3. Statement of Intent 5
4. General Statement of Scope 6
5. Roles and Responsibilities 6
   - 5.1 Responsibilities of every user of The Companies IT resources 6
     - 5.1.1 Appropriate use of IT resources 6
     - 5.1.2 Confidentiality of passwords 6
   - 5.2 Responsibilities specific to every staff member of The Companies 6
     - 5.2.1 Appropriate use of IT resources 6
     - 5.2.2 Asking for help, reporting a concern 6
   - 5.3 Responsibilities specific to managers 6
     - 5.3.1 Fully understand the data, people, systems and processes 6
     - 5.3.2 Setup resilient business processes 7
     - 5.3.3 Oversee their teams and systems are effective 7
     - 5.3.4 Monitor the 3rd party with access to The Companies systems and data 7
   - 5.4 Responsibilities of senior management 7
     - 5.4.1 Risk ownership 7
     - 5.4.2 Risk Acceptance 7
     - 5.4.3 Risk Treatment 7
     - 5.4.4 Policies and education 7
     - 5.4.5 Incident response 7
   - 5.5 Responsibilities specific to 3rd party providers 8
     - 5.5.1 Meeting terms of service/contract agreements, right to audit. 8
6. Policy 8
   - 6.1 Organisation of information security 8
     - 6.1.1 Ultimate accountability for security 8
     - 6.1.2 Information security reviews 8
     - 6.1.3 Information Security Manager 8

6.1.4 Segregation of duties 8
6.2 Policy management, education and awareness 8
6.2.1 Policies as minimum expectation, need for risk management 8
6.2.2 Policy issuing, communication and updating 9
6.2.3 Trust, but verify 9
6.2.4 Awareness and education on policies and procedures 9
6.3 HUMAN RESOURCE SECURITY 9
6.3.1 Acceptable use of UWL resources 9
6.3.2 Responsibility for reporting non-compliance 9
6.3.3 Management responsibility for security 9
6.3.4 Background checks on employees 9
6.3.5 Terms and condition of employment 9
6.3.6 Enforcement of information security policies 10
6.4 Data / assets management 10
6.4.1 Data classification 10
6.4.2 Retention of information 10
6.4.3 Safe storage, use and disposal of electronic media and surplus hardware 10
6.4.4 Use of removable media 11
6.4.5 Physical security, controlled areas 11
6.5 Security by design, secure architecture, acquisition and development 11
6.5.1 Governance on approved technology and security design principles 11
6.5.2 Information security in new projects 11
6.5.3 Separation of Environments 11
6.5.4 Protection from malware 11
6.5.5 Minimum security features in systems 12
6.5.6 Installation of software, patching 12
6.5.7 Testing of security 12
6.6 Technical and operational security 12
6.6.1 Control requirements for remote and mobile access / working 12
6.6.2 Encryption of data 12
6.6.3 Logging and auditing 12
6.6.4 Physical and environmental security 12
6.6.5 Data backup and restore procedures 13
6.7 Access management 13
6.7.1 Due diligence before granting access 13

6.7.2 User accountability for security 13
6.7.3 Privileged access to systems 13
6.8 Incident management 13
6.8.1 Incident response 13
6.8.2 Contact with authorities 13
6.8.3 Responsibilities of staff 13
6.9 Continuity management 13
6.9.1 Secure operations in contingency 13
6.9.2 Business management responsibility for security 14
6.10 Compliance, validation and certification 14
6.10.1 Compliance with the law 14
6.10.2 Information security in contracts with 3rd parties 14
6.10.3 Supplier service delivery management 14
6.10.4 Management controls 14
6.10.5 Internal and independent security reviews 14

1. Document Control

Document owner	Serena Fordham Managing Director and Founder
Prepared by	John Fordham Glow Virtual Assistants Operation Manager
Reviewed by	Serena Fordham Managing Director and Founder
Approved by	Serena Fordham Managing Director and Founder
Approved on	1st May 2018 (Updated 30th October 2018)
Next review date	1st April 2019
Reference	ISP_002
Version	1.0
Classification	Public

Distribution list	
Managing Director	To approve and authorise
All Staff	To understand and comply

Communication	The Information Security Policy is communicated to all members of staff via email and information security awareness training.

2. Introduction

Serena Fordham Enterprises Limited, For HER Group Limited and Norfolk Mums ('The Companies') is registered with the Information Commissioners Office (ICO).

The Companies have an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information The Companies are responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

This Information Security Policy outlines The Companies approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of data and information systems.

The Companies consider information to be a strategic asset that is essential to its core business and objectives. It has a responsibility to manage effectively the risks around protecting the confidentiality, integrity and availability of its data and in complying with all statutory, regulatory and legal requirements.

The Companies recognise the General Data Protection Regulation (GDPR) and will endeavour to ensure that all personal data is stored and processed in compliance with this regulation from 25 May 2018, the date the regulation comes into force.

3. Statement of Intent

The main purpose of this Policy is to describe the minimum level of protection that The Companies expects of all The Companies information systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

A secondary but very relevant purpose of this Policy is to ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle, including making users aware of relevant legislation.

The overarching objectives set out in the Policy are:

- To support the business objectives in a flexible and effective way
- To maintain adequate regulatory compliance
- To protect The Companies information assets
- To maintain business continuity

The policy of The Companies is to protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.

The Companies Senior Management will ensure business, legal, regulatory requirements and contractual information security obligations are met.

Information security management system will be monitored regularly with reporting of the status and effectiveness at all levels.

4. General Statement of Scope

This Policy is applicable, and will be communicated to all staff of The Companies and The Companies clients who interact with information held by The Companies and the information systems used to store and process it.

5. Roles and Responsibilities

5.1 Responsibilities of every user of The Companies IT resources

5.1.1 Appropriate use of IT resources

The Companies staff and any other authorised users of The Companies IT resources are expected to meet the acceptable usage policies and related terms and conditions of the services provided by The Companies and by any 3rd party on our behalf under licensing agreements.

5.1.2 Confidentiality of passwords

Users must manage passwords with care and processes should be in place to ensure confidentiality from the initial creation, storage in applications, communication and day to day usage.

5.2 Responsibilities specific to every staff member of The Companies

5.2.1 Appropriate use of IT resources

All employees and any third parties authorised to use The Companies systems are accountable for understanding and following The Companies information security policies, as well as promoting safe practices within their teams and monitor compliance.

5.2.2 Asking for help, reporting a concern

All employees and authorised third parties are responsible for asking for assistance when in doubt about how to proceed or interpret a policy and also to report any concern or suspect activity encountered.

5.3 Responsibilities specific to managers

5.3.1 Fully understand the data, people, systems and processes

The Companies managers are expected to identify the data and systems under their remit and, where appropriate and reasonable, accept accountability for its protection. Managers will make informed decisions on risks and appropriate levels of protection, on behalf of The Companies.

5.3.2 Setup resilient business processes

The Companies managers should ensure that risks are mitigated through the introduction of resilient and robust business processes. Managers should ensure that they and their teams (where appropriate) are security savvy, ensuring that responsibilities regarding protecting systems and data are adequately communicated.

5.3.3 Oversee their teams and systems are effective

The Companies managers should actively, regularly and demonstrably verify what their reports are doing and how systems under his/her supervision are functioning.

5.3.4 Monitor the 3rd party with access to The Companies systems and data

The Companies managers should ensure any subcontractor employed for a particular function will meet the requirements specified (on selection and on an ongoing basis) and accept responsibility for their actions.

5.4 Responsibilities of senior management

5.4.1 Risk ownership

The Managing Director owns the overall risk management process, and the prioritisation and acceptance of risks. Risks are generally identified "bottom up" from each staff member and "top down" from the Managing Director in a two-way flow.

5.4.2 Risk Acceptance

The Companies managers have the accountability for taking a stance on risks within their authority (or escalating if exceeds it) and ensuring the business operates in line with the Managing Director's expectations and within regulation.

5.4.3 Risk Treatment

All The Companies staff will help to identify and mitigate risks. The Managing Director will take advice from these and other sources in assessing and managing risk. Ultimately, the responsibility for risk lies with the Managing Director.

5.4.4 Policies and education

The Managing Director and managers are responsible for communicating acceptable levels of risk and mitigation practices to all The Companies staff and authorised 3rd parties via policy, standards and awareness programs.

5.4.5 Incident response

The Managing Director and managers are responsible for effectively responding to significant information security related incidents.

5.5 Responsibilities specific to 3rd party providers

5.5.1 Meeting terms of service/contract agreements, right to audit.

3rd party shall adhere to the IT acceptable usage policy as well as any other requirements specified in the service contract.

6. Policy

6.1 Organisation of information security

6.1.1 Ultimate accountability for security

The Managing Director has the ultimate accountability for implementing information security at The Companies.

6.1.2 Information security reviews

A regular review of information security shall be established and led by the Managing Director. The review will be completed annually.

The Managing Director and all The Companies staff will review and discuss information security issues at regular team meeting, including delivering policy and awareness training / updates.

6.1.3 Information Security Manager

It is not currently appropriate for The Companies to have the role of Information Security Manager due to the small scale of the business.

6.1.4 Segregation of duties

Conflicting duties and areas of responsibility are unlikely to arise given the current small scale of The Companies, with the exception of clients and staff matters / payments which are currently handled solely by the Managing Director. However, it is recognised by The Companies that duties should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the business assets.

6.2 Policy management, education and awareness

6.2.1 Policies as minimum expectation, need for risk management

Managing risks is an essential part of the business activity at all levels of management. The information security policies are the minimum expectation to address information security risks according to well established practice.

Management should assess the business, legal, contractual and corporate social responsibility risks and requirements in each relevant jurisdiction to decide on the need for additional controls or exceptions, and be able to justify and be accountable for these decisions.

6.2.2 Policy issuing, communication and updating

Policies and procedures for information security and data protection will be maintained, approved by management, published and communicated to employees and relevant authorised external parties. These Policies should be reviewed and updated at least annually.

6.2.3 Trust, but verify

The Policy statements are necessary but not sufficient on their own. The Companies staff should demonstrate the application of the controls and best practice.

6.2.4 Awareness and education on policies and procedures

The Managing Director and managers should ensure staff and external authorised parties working with The Companies systems and data are formally aware of and educated on the policies and procedures they must be compliant with. This is a fundamental step to establishing any individual's accountability.

6.3 HUMAN RESOURCE SECURITY

6.3.1 Acceptable use of UWL resources

Every employee and authorised 3rd party granted access to The Companies systems and/or data has a responsibility to use the systems and data in a secure manner, for The Companies business purposes, following The Companies policies and applying good judgment. Only approved hardware, software and data should be used to perform The Companies business, unless otherwise agreed.

6.3.2 Responsibility for reporting non-compliance

Users are responsible for reporting any concern on how the security processes are performing, any suspected or confirmed incident regarding unauthorized or incorrect use to their manager.

6.3.3 Management responsibility for security

Management is responsible for requiring their teams (where applicable) and contractors to apply information security according to established policies and procedures, and to monitor use within his/her teams, leading by example and ensuring their direct reports have been educated on policies and security practices.

6.3.4 Background checks on employees

The Companies are not of a scale to warrant checks on prospective employees. In general, existing employees have previously been known to the business and Managing Director.

6.3.5 Terms and condition of employment

The contractual agreements with employees and contractors shall state their responsibilities for data protection and information security.

6.3.6 Enforcement of information security policies

The Managing Director is responsible for defining and communicating the disciplinary process applicable to employees who have committed an information security breach.

6.4 Data / assets management

6.4.1 Data classification

Each manager must identify the data being used for fulfilling their duties and adopt processes appropriate to protect the information according to its risk. It should be assumed that all information is critical.

6.4.2 Retention of information

The Companies will have processes in place to safely dispose of information as required by law or, within legal compliance, when it is no longer necessary to retain. Generally, the only data stored by The Companies, is stored electronically on local laptops, or stored with 3rd party software providers. When electronic data is required to be deleted, this is completed locally from laptops ensuring that all relevant data is removed, or is completed via the 3rd party software following their standard deletion routines.

In the rare instances that hard copy data is collected, it is the accepted practice to transfer the data to electronic systems with the original hard copy being destroyed / shredded. Where this practice is not appropriate and hard copies are retained, these are stored in a locked filing cabinet within a locked office.

Retention periods are generally defined by the Managing Director (for The Companies staff and client payment related data) and by the clients of The Companies (for client customer and prospective customer data), but always in accordance with the relevant regulation.

6.4.3 Safe storage, use and disposal of electronic media and surplus hardware

Currently The Companies operating model is that each staff member is responsible for providing their own electronic media and hardware. Therefore, it is the staff members responsibility to securely store and dispose of media and hardware using best practice, such as:

Storage, use:

- Devices to be password protected.
- Individual files to be password protected.
- Devices to be stored securely when not in use, out of direct sight of windows etc.
- Operating system to be kept updated with manufacturer recommended updates.
- Only manufacturer approved and recommended software updates to be applied.
- Operating system firewall to be turned on.
- Anti-virus protection to be installed.
- Regular sweeps for virus and malware to be conducted.

Disposal:

- Device to be reset to factory settings to eliminate all traces of data.
- Where possible, hard drive to be removed for destruction.

The Companies recognise the environmental impacts of the disposal of media and hardware and would employ best practice at the time of disposal to limit the impact. Arrangements need to be dealt with on a case by case basis.

6.4.4 Use of removable media

The Companies accept that in certain circumstances the use of removable media is necessary. Where this use is defined as being required, the media device should be rest to factory settings before and after use (to remove all traces of previous / current data). The use of encryption will be considered on a case by case basis. The removable media is to be securely stored.

6.4.5 Physical security, controlled areas

As referred to in 6.4.3 The Companies require each staff member to ensure security of their hardware, systems and media, protecting them against intentional or accidental physical damage. Each staff member generally works remotely and as such The Companies do not have a single site requiring physical security or controlled areas.

6.5 Security by design, secure architecture, acquisition and development

6.5.1 Governance on approved technology and security design principles

Should the use of new technology be required in a specific project or assignment, generally the Managing Director will determine if the suggested approach and technologies are acceptable for The Companies.

6.5.2 Information security in new projects

Information security shall be considered for any new project which falls outside of the standard processing techniques or systems.

6.5.3 Separation of Environments

Due to the nature of the current The Companies business models, system environments, for example test and production, are not required.

6.5.4 Protection from malware

As referred to in 6.4.3 the default approach is that all The Companies hardware should have detection, prevention and recovery controls to protect against malware combined with appropriate user awareness. Exceptions need to be formally approved on a case by case basis by the Managing Director.

6.5.5 Minimum security features in systems

Systems should be developed/acquired and configured with the security features necessary to enable enforcement of the following:

- Staff and authorised users can only access data and functionality for which they are authorised.
- Accountability for usage is maintained via appropriate audit trails.

6.5.6 Installation of software, patching

As referred to in 6.4.3 manufacturer approved / recommended software updates should be kept current. To facilitate this, 'updates' should always be set to auto-update.

6.5.7 Testing of security

Whilst The Companies have no formal security testing procedure, staff are aware that periodically senior staff may undertake testing of security as part of the regular business as usual.

6.6 Technical and operational security

6.6.1 Control requirements for remote and mobile access / working

The Companies staff generally operate remotely and therefore as such there are no additional control requirements for remote access.

With regards to mobile access and working, staff are required to be aware of their surroundings and take any appropriate measures to ensure security, including but not limited to, the physical security of the hardware and data.

6.6.2 Encryption of data

The Companies do not currently regularly encrypt data unless it is required for specific projects. Data is generally transferred electronically through known channels / systems. Where there are exceptions to this, the circumstances and need for encryption will be determined on a case by case basis.

6.6.3 Logging and auditing

As such, The Companies do not actively log or audit systems use due to the nature of the business model as previously described. Therefore, only manufacturer, software or 3rd party logging is completed. For example, website hosting provided by third parties maintains an audit of changes to pages and content.

6.6.4 Physical and environmental security

As previously described in this Policy, it is the responsibility of staff to provide physical and environmental security for devices, hardware and hard copies of data. Exceptions to this are considered on a case by case basis.

6.6.5 Data backup and restore procedures

A 3rd party storage provider (currently "DropBox") is used by The Companies for the storage of the majority of client files. Other data, for example client customer data, is stored on a variety of other 3rd party systems and these will maintain their own backups.

System backups and restore procedures are not performed explicitly by The Companies, rather, these are inherent in the operating systems and software employed by the business.

6.7 Access management

6.7.1 Due diligence before granting access

Access to systems and information, including setting up permanent network connectivity solutions, will be granted to employees and third parties/service providers only after a due diligence assessment has been performed and after the employment or service contracts, including confidentiality and accountability clauses has been agreed in writing.

6.7.2 User accountability for security

All employees and third parties using The Companies systems are accountable for understanding and following The Companies security policies, in particular on how to protect their accounts and passwords from misuse. All employees are expected to report any concern or potential suspect activity they may encounter.

6.7.3 Privileged access to systems

All privileged/administrator activity (e.g., providing access to data, maintenance, and support) will be traceable to the individuals through the 3rd party software / system providers routines.

6.8 Incident management

6.8.1 Incident response

The Companies incident management will be maintained by the Managing Director or the manager designated for dealing with such incidents. The incident response will be determined on a case by case basis.

6.8.2 Contact with authorities

Appropriate contacts with relevant authorities and external parties shall be maintained. In case of an incident, contacts will be nominated who are authorised to liaise with authorities and external parties.

6.8.3 Responsibilities of staff

If a member of The Companies staff is aware of an information security incident then they must report it to the Managing Director.

6.9 Continuity management

6.9.1 Secure operations in contingency

People, assets and information services need to be protected in a disaster situation. Should such situations arise, each will be treated on a case by case basis.

6.9.2 Business management responsibility for security

The Companies staff are responsible for security and, where appropriate, the availability of systems/data.

6.10 Compliance, validation and certification

6.10.1 Compliance with the law

The Companies and each of their employees is accountable for operating within the law, and it is their responsibility to be aware of legal and contractual requirements and implement the controls within their remits to comply.

6.10.2 Information security in contracts with 3rd parties

The Companies contracts with 3rd parties, including contracts with The Companies clients, will contain appropriate security and regulatory or contractual obligations. Where The Companies has no powers to set or amend the contractual wording of 3rd party providers, the appropriateness of each contract will be considered on a case by case basis.

6.10.3 Supplier service delivery management

The Companies Managing Director and / or staff members assume responsibility for monitoring and reviewing supplier service delivery where this is appropriate.

6.10.4 Management controls

When appropriate, The Companies managers should review the compliance of information processing and procedures within their area of responsibility with this security policy.

6.10.5 Internal and independent security reviews

Internal security reviews may be undertaken at the instruction of the Managing Director. Independent security reviews are considered unlikely to be required given the current The Companies business models, however they remain an option should an appropriate situation arise.